P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

ANALISIS KOMBINASI ALGORITMA KRIPTOGRAFI RSA DAN ALGORITMA STEGANOGRAFI *LEAST SIGNIFICANT BIT (LSB)* DALAM PENGAMANAN PESAN DIGITAL

Taufik Ryan Kuncoro[1,a)] R. Aditama[2,b)]
[1]Program Studi Matematika FMIPA Universitas Pamulang
[2]Program Studi Matematika FMIPA Universitas Pamulang
Email: [a)]taufikryan12@gmail.com [b)]adi.n6ts@gmail.com

ABSTRACT

Cryptography and steganography are methods that have different scheme to hide an information. Cryptography is a method to encode an information becomes any codes that other people not easy to understand, and steganography is a method to hide an information into some medium. In this paper has been developed a combining algorithm of cryptography and steganography scheme. It used RSA cryptography algorithm and LSB steganography algorithm. The analysis of this combined algorithm includes an analysis of time process, the similarity of the image after the process, and the security or message when stego image was edited and also when image sent by messaging tools. After the analysis and implementation of combine algorithm have done, we know that RSA cryptography algorithm can be used in combination with LSB steganography algorithm to secure digital message. After the test of data has done, we get the result that the message has been hidden can be resolved perfectly. The faster time process is 0.09 seconds and the slowest is 1.285 seconds. The smalest PSNR value is 53.0696 dB and the bigest is 66.2185 dB. The image that use to hide an encrypted message has to save in bitmap without any editing and able to send by e-mail and line so that secret message is still remains intact.

Keywords: Cryptography, Least Significant Bit, RSA, Steganography.

ABSTRAK

Kriptografi dan Steganografi merupakan ilmu yang digunakan untuk merahasiakan informasi dengan prinsip yang berbeda. Kriptografi yaitu sebuah metode untuk menyandikan informasi menjadi kode-kode yang tidak dengan mudah dimengerti oleh orang-orang yang tidak berkepentingan, dan steganografi adalah metode untuk menyembunyikan informasi ke dalam suatu media. Dalam skripsi ini dikembangkan sebuah algoritma kombinasi dari skema kriptografi dan steganografi. Algoritma yang digunakan adalah algoritma Kriptografi RSA dan algoritma Steganografi LSB. Analisis yang dilakukan terhadap kombinasi algoritma dalam skripsi ini meliputi analisis terhadap waktu proses, tingkat kesamaan citra digital setelah proses, dan keamanan informasi ketika dilakukan perubahan pada citra digital serta pengiriman media melalui aplikasi tertentu. Setelah dilakukan analisis dan implementasi terhadap kombinasi kedua metode tersebut, didapat bahwa algoritma kriptografi RSA dapat digabungkan dengan algoritma steganografi LSB dalam pengamanan pesan digital. Setelah dilakukan pengujian terhadap data didapat bahwa pesan yang dirahasiakan dapat kembali diperoleh secara utuh. Waktu

StatMat
Jurnal Statistika dan Matematika
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

proses tercepat yang diperlukan adalah 0.09 detik dan yang terlama adalah 1.285 detik. Nilai PSNR terkecil 53.0696 dB dan nilai terbesar adalah 66.2185 dB. Citra digital yang digunakan untuk menyimpan hasil enkripsi harus disimpan dalam bentuk citra bitmap tanpa dilakukan perubahan terhadap citra dan dapat dikirim dengan menggunakan e-mail dan line agar pesan rahasia tetap utuh.
Kata kunci: Analisis Kriptografi, Least Significant Bit, RSA, Steganografi.

1. PENDAHULUAN

Komunikasi merupakan salah satu aktivitas mendasar dan utama yang pasti dilakukan manusia. Dengan komunikasi manusia dapat berhubungan dengan orang lain di dalam kehidupan dan kegiatan yang dilakukan sehari-hari. Pada zaman yang semakin modern ini, teknologi berperan besar dalam komunikasi maupun penyampaian informasi. Semakin berkembangnya kebutuhan manusia dalam berkomunikasi, semakin tinggi pula permintaan yang berkaitan dengan kelengkapan fitur pada alat komunikasi yang digunakan. Diantara banyaknya fitur yang diinginkan, salah satunya adalah mengenai keamanan agar privasi informasi dapat terpenuhi.

Dalam kegiatan yang dianggap penting seperti transaksi ekonomi, bisnis, penyimpanan barang berharga, dan data rahasia pribadi sangat membutuhkan keamanan yang tinggi agar pihak yang bersangkutan tidak dirugikan. Meskipun informasi yang disampaikan tidak secara langsung ditunjukkan kepada pihak lain, namun tetap ada kemungkinan informasi tersebut tersebar bebas tanpa diketahui oleh pihak terkait. Salah satu penyebab bocornya informasi adalah karena lemahnya sistem keamanan, algoritma yang sederhana, gangguan virus, atau serangan yang disengaja dari pihak lain. Adapun langkah yang dapat dilakukan dalam berkomunikasi tanpa tersadap oleh pihak lain yaitu kedua pihak yang saling berkomunikasi dapat melakukan perjanjian dalam menggunakan kode atau simbol tertentu yang hanya diketahui oleh pihak terkait yang disampaikan dengan metode yang telah disepakati bersama. Banyak organisasi ataupun individu yang tidak ingin informasi yang disampaikannya diketahui oleh kompetitor ataupun pihak lain yang tidak memiliki kepentigan. Oleh karena itu dikembangkan berbagai ilmu pengetahuan yang mempelajari tentang bagaimana cara pengamanan data, dianntaranya adalah kriptografi dan steganografi.

Teknik kriptografi dapat mengubah pesan rahasia menjadi pesan acak *(ciphertext)* yang tidak memiliki makna sehingga pesan rahasia hanya dapat terbaca oleh pihak yang berhak, namun teknik ini memiliki kelemahan yaitu pesan acak yang ditampilkan dapat menimbulkan kecurigaan sehingga memungkinkan pelaku kejahatan untuk memanipulasi serta memodifikasi pesan acak *(ciphertext)* yang mengakibatkan pesan rahasia menjadi rusak.

Teknik lain yang dapat digunakan untuk melindungi pesan rahasia adalah dengan menggunakan steganografi yaitu teknik menyembunyian pesan rahasia ke dalam media digital sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Steganografi

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

adalah seni menyembunyikan informasi untuk mencegah pendeteksian pesan yang disembunyikan dengan cara meyisipkan pesan rahasia kedalam media gambar, audio dan lain lain, namun dengan menggunakan teknik ini-pun tidak menjamin bahwa pesan rahasia benar benar terlindungi dari pelaku kejahatan.

Salah satu cara untuk mengatasi kedua permasalahan tersebut adalah dengan menggunakan kombinasi antara kriptografi dan steganografi. Teknik kriptografi bekerja menyandikan pesan rahasia yang akan diubah menjadi pesan acak *(ciphertext)* dan steganografi bekerja menyisipkan pesan acak *(ciphertext)* kedalam sebuah media *(cover object).*

Dalam Skripsi ini akan dilakukan penelitian pengamanan pesan digital dengan algoritma kriptografi RSA (Rivest Shamir Adleman), yang dikombinasikan dengan metode steganografi LSB *(Least Significant Bit)*. Penelitian ini dilakukan dengan menggunakan bantuan software Matlab R2015a.

2. METODOLOGI PENELITIAN

Penelitian ini dilaksanakan di Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Pamulang Tangerang Selatan mulai bulan Juni 2018. Metode penelitian yang dilakukan oleh peneliti adalah studi literatur. Peneliti membaca buku-buku dan jurnal-jurnal yang berkaitan dengan kriptografi, steganografi dan pengolahan citra. Tujuan dari studi literatur adalah untuk memperoleh sumber referensi yang berisi teori-teori serta penelitian-penelitian yang telah dilakukan sebelumnya guna memberikan kemudahan dalam melakukan penelitian ini.

Dalam penelitian analisis kombinasi algoritma kriptografi RSA dan algoritma steganografi *least significant bit (LSB)* dalam pengamanan pesan digital ini peneliti menggunakan perangkat guna mendukung kelancaran penelitian yang dilakukan. Perangkat pendukung disini meliputi perangkat keras *(hardware),* dan perangkat lunak *(software).*

Perangkat keras yang digunakan peneliti adalah satu unit laptop dengan spesifikasi sebagai berikut:

a. *Processor* : Intel(R) Core(TM) i3-4005U CPU @ 1.70GHz
b. *Memory* : 4096 MB RAM.
c. *DirectX Version* : DirectX 12.
d. *Chip Type* : Intel(R) HD Graphics 2124MB.
e. *Graphics Card* : AMD Radeon Graphics Processor 4051MB.

Sedangkan perangkat lunak yang digunakan peneliti dalam penelitian ini adalah sebagai berikut :

a. *Operating System* : Windows 10 Pro 64-bit (10.0, Build 16299)
b. Matlab R2015a.
c. Adobe Photoshop CS6.

StatMat
Jurnal Statistika dan Matematika
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

Untuk analisis algoritma serta perancangan sistem mengikuti langkah-langkah berikut ini:

a. Enkripsi dan Dekripsi RSA

Algoritma RSA didasarkan pada teorema euler yang menyatakan bahwa:

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n) \qquad (2.1)$$

yang dalam hal ini :

1. α harus relatif prima terhadap *r*.
2. $\varphi(n) = r(1-1/p_1)\ (1-1/p_2)\ldots\ (1-1/p_i)$, yang dalam hal ini $p_1, p_2, \ldots, p_i$ adalah faktor-faktor prima dari *n*.

Setelah memahami teorema euler, maka kemudian dijabarkan mengenai penerapan teorema euler dalam proses pembentukan rumus untuk enkripsi dan juga dekripsi dari algoritma RSA.

Dari teorema euler didapatkan sebuah persamaan $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$. Dimana α harus relatif prima terhadap *n*. Kemudian digunakan notasi P untuk menggantikan α, dimana notasi P merupakan *plaintext.*

$$P^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n) \qquad (2.2)$$

Berdasarkan sifat $a^m \equiv b^m (\mathrm{mod}\, n)$ untuk *m* bilangan bulat ≥ 1, maka persamaan (2.2) dapat ditulis menjadi :

$$P^{m\varphi(n)} \equiv 1 (\mathrm{mod}\, n) \qquad (2.3)$$

Berdasarkan sifat $ac \equiv bc (\mathrm{mod}\, n)$ maka bila persamaan (2.3) dikali dengan P akan mejadi:

$$P^{m\varphi(n)+1} \equiv P (\mathrm{mod}\, n) \qquad (2.4)$$

yang dalam hal ini P relatif prima terhadap *n.*

Misalkan *e* dan *d* (yang nantinya digunakan sebagai kunci enkripsi dan kunci dekripsi) yang telah ditentukan sedemikian sehingga :

$$e.d \equiv 1 (\mathrm{mod}\, \varphi(n)) \qquad (2.5)$$

atau

$$e.d \equiv m\varphi(n) + 1 \qquad (2.6)$$

Persamaan (2.6) ini nantinya yang digunakan untuk pembangkitan pasangan kunci. Persamaan (2.4) disubtitusikan ke dalam persamaan (2.6), menjadi :

$$P^{ed} \equiv P (\mathrm{mod}\, n) \qquad (2.7)$$

Persamaan (3.7) dapat ditulis kembali menjadi :

$$(P^e)^d \equiv P (\mathrm{mod}\, n) \qquad (2.8)$$

Yang artinya, perpangkatan P dengan *e* diikuti dengan perpangkatan dengan *d* menghasilkan kembali P semula.

StatMat
Jurnal Statistika dan Matematika
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

Berdasarkan persamaan (3.8), maka enkripsi dan dekripsi dirumuskan sebagai berikut:

Enkripsi (P) = $C \equiv P^e \pmod n$ (2.9)

Dekripsi (C) = $P \equiv C^d \pmod n$ (2.10)

b. Pembangkit Pasangan Kunci

Sebagai algoritma Asimetris Kriptografi, RSA membutuhkan dua kunci yang berbeda untuk enkripsi dan dekripsi. Bilangan yang dipilih sebagai kunci adalah bilangan prima yang besar, dengan alasan pemfaktoran sebuah bilangan hasil perkalian dari dua bilangan prima yang besar menjadi dua bilangan prima yang sesuai akan sangat sulit. Sehingga keamanan dari RSA dapat terjamin.

Pasangan kunci merupakan suatu komponen penting dalam kriptografi RSA. Untuk membangkitkan kedua kunci dipilih dua bilangan prima acak yang besar. Sehingga terjadi pemfaktoran bilangan yang sangat besar, karena alasan tersebut RSA dianggap aman.

Berikut ini langkah-langkah proses pembangkitan pasangan kunci :

1) Dipilih dua buah bilangan prima sembarang, *p* dan *q*
2) Dihitung nilai *n=p.q*
3) Nilai totient dari *n* yang disimbolkan φ*(n)* dapat dihitung menggunakan Fungsi φ Euler.
4) Dipilih bilangan *e*, dimana *e* relatif prima terhadap φ*(n)* . Bilangan yang relatif prima adalah bilangan yang memiliki Faktor Persekutuan Terbesar atau *Greatest Common Divisor (GDC)* sama dengan 1. Hal ini dapat ditentukan dengan menggunakan proses Algoritma Euclide.
5) Ditentukan bilangan *d* dengan persamaan (2.6).

Perhatikan $e.d \equiv m\varphi(n)+1$, sehingga *d* dapat dihitung dengan

$$d = \frac{1+m\varphi(n)}{e} \qquad (2.11)$$

Dimana *m=1,2,3,…,* sehingga diperoleh nilai *d* yang bulat dengan demikian :

kunci umum adalah pasangan *(e, n)*

kunci rahasia adalah pasangan *(d, n)*

c. Embedding dan Ekstraksi

Konsep dasar dari subtitusi LSB adalah dengan menggantikan data rahasia di paling kanan bit (bit dengan bobot terkecil) sehingga prosedur embedding tidak signifikan mempengaruhi nilai piksel aslinya. Representasi matematika pada metode LSB adalah:

$$I_s(x,y) = \begin{cases} I(x,y) - 1 & LSB(I(x,y))=1 \text{ , } m=0 \\ I(x,y) & LSB(I(x,y))=m \\ I(x,y)+1 & LSB(I(x,y))=0 \text{ , } m=1 \end{cases} \qquad (2.12)$$

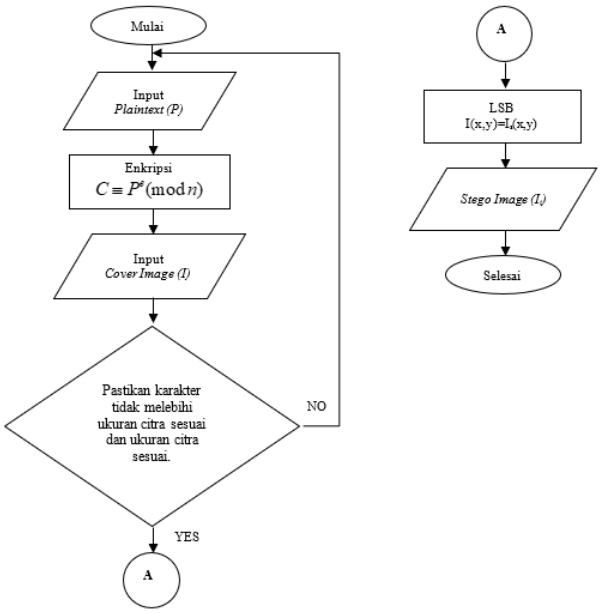
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

Fungsi di atas menggambarkan bahwa I(x, y) merupakan nilai piksel dari sebuah citra, m menggambarkan bit pesan yang akan disisipkan, dan LSB(I(x, y)) merupakan bit terakhir pada piksel.

Implementasi penelitian ini yaitu menerapkan kombinasi antara metode kriptografi RSA dengan metode steganografi LSB untuk mendapatkan keamanan yang tinggi guna melindungi pesan rahasia sampai tujuan dengan aman dan utuh. Dalam implementasi ini, pesan rahasia yang akan digunakan adalah teks digital, sedangkan format file *cover image* yang berperan sebagai wadah menggunakan format file (.jpg/.jpeg). Pertama pesan rahasia *(plaintext)* akan dienkripsi menggunakan kunci umum sehingga didapatkan pesan acak *(ciphertext)*, selanjutnya *ciphertext* diubah bentuknya menjadi bentuk biner untuk disisipkan pada *cover image* menggunakan skema *Least Significant Bit (LSB).* Proses ekstraksi berkas dengan cara memasukkan *stegoimage* yang dihasilkan dari proses penyisipan untuk mendapatkan berkas *ciphertext* dan selanjutnya *ciphertext* di dekripsi guna mendapatkan pesan rahasia atau *plaintext.* Implementasi sistem ini dibangun menggunakan software Matlab R2015a. Adapun Implementasi dilalui melalui 2 tahapan yakni:

a. Proses Ekstraksi dan Dekripsi

Proses ini adalah proses pengembalian pesan ke bentuk awal, *stego image* akan diekstrak kembali untuk mendapatkan *ciphertext* yang tersembunyi yang kemudian *ciphertext* akan didekripsi untuk mendapatkan pesan rahasia *(plaintext).* Adapun tahapan yang dilakukan penerima dalam proses ekstraksi sampai dekripsi adalah sebagai berikut



Gambar 2. 1 Alur Enkripsi dan Embeding (Penyisipan Berkas)

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

1) *Plaintext*

   Plaintext merupakan pesan rahasia yang akan dikirim kepada penerima dan wajib dijaga kerahasiaannya. Pada proses ini pengirim memasukkan pesan rahasia kedalam sistem untuk disandikan menjadi bentuk yang tidak dimengerti.

2) Proses Enkripsi

   Pada proses ini dilakukan penyandian pesan rahasia ke dalam bentuk pesan yang tidak memiliki pola sehingga pesan rahasia menjadi tersamarkan. Proses ini dilakukan oleh sistem menggunakan metode kriptografi RSA yang akan menghasilkan output berupa *ciphertext.*

3) Melakukan *Input Cover Image*

   Pada proses ini pengirim memasukkan gambar ke dalam sistem sebagai media penampung. Gambar yang akan dijadikan *cover image* harus memiliki format (.jpeg/jpg). Format file (.jpeg/jpg) dipilih dikarenakan format ini merupakan format yang paling umum serta paling banyak digunakan dalam file citra digital.

4) Verifikasi *Cover Image* dan Berkas *Ciphertext*

   Sistem melakukan proses verifikasi yang berguna untuk menjaga kekonsistenan pada hasil berupa *stego image.*

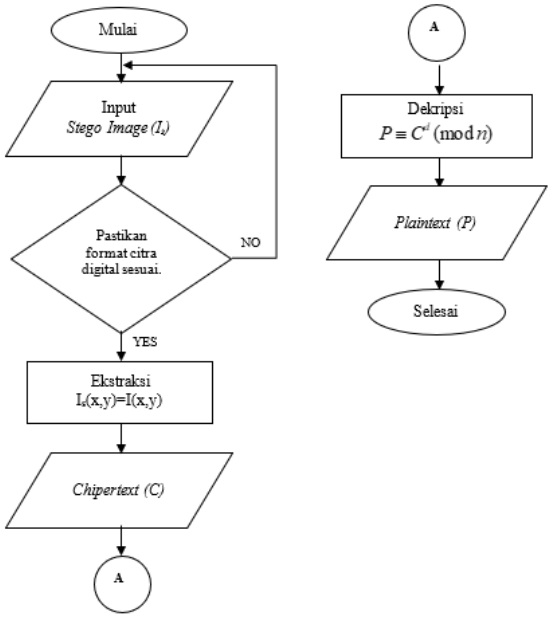
5) Proses Penyisipan Berkas

   Penyisipan berkas dilakukan oleh sistem dengan menggunakan metode steganografi LSB, sehingga menghasilkan output berupa stegoimage yang di dalam-nya terkandung pesan rahasia. *Stego image* memiliki format citra bitmap (.png) dikarenakan format tersebut baik dalam akurasi penyimpanan data

b. Proses Ekstraksi dan Dekripsi

Proses ini adalah proses pengembalian pesan ke bentuk awal, *stego image* akan diekstrak kembali untuk mendapatkan *ciphertext* yang tersembunyi yang kemudian *ciphertext* akan didekripsi untuk mendapatkan pesan rahasia *(plaintext).* Adapun tahapan yang dilakukan penerima dalam proses ekstraksi sampai dekripsi adalah sebagai berikut.

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam



Gambar 2. 2 Alur Ekstraksi dan Dekripsi

1) Melakukan *Input Stegoimage*

   Stegoimage merupakan media gambar yang mengandung pesan rahasia. Pada proses ini penerima memasukkan *stegoimage* yang telah didapatkan oleh pengirim kedalam sistem.

2) Verifikasi *Stegoimage*

   Proses verifikasi *stegoimage* dilakukan oleh sistem untuk memverifikasi format stegoimage yang dimasukkan penerima memiliki format citra bitmap (.png).

3) Proses *Ekstraksi*

   Pada proses ini dilakukan pengembalian berkas dengan menggunakan metode steganografi LSB dengan output berupa berkas *ciphertext.*

4) Proses Dekripsi

   Proses dekripsi dilakukan oleh sistem menggunakan metode kriptografi RSA. Proses ini berfungsi mengembalikan ke bentuk semula dari pesan acak atau *ciphertext* yang dimasukkan oleh penerima menjadi pesan rahasia atau *plaintext.*

Tahap terakhir adalah pengujian atau *testing* adalah tahap untuk memastikan seluruh kebutuhan yang telah diimplementasikan bekerja semestinya serta mengidentifikasi kekurangan pada sistem. Pada tahap ini terdapat beberapa hal yang akan dilakukan pengujian yaitu:

a. Pengujian Enkripsi dan Dekripsi

   Pengujian ini dilakukan untuk membuktikan apakah proses enkripsi pesan rahasia dapat diubah kedalam bentuk yang tidak dimengerti maknanya dan sebaliknya pada saat dekripsi, apakah pesan yang tidak bermakna tersebut berhasil dikembalikan kedalam bentuk yang memiliki makna sesuai dengan aslinya tanpa mengurangi, menambah, dan memodifikasi isinya.

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

b. Pengujian Waktu Proses
   Pengujian ini dilakukan untuk mengetahui waktu proses program, baik dalam proses enkripsi-embedding maupun proses ekstraksi-dekripsi. Pengujian ini bertujuan untuk mengetahui pengaruh ukuran data terhadap lamanya waktu proses yang diperlukan.
c. Pengujian Tingkat Kemiripan *Cover Image* dan *Stego Image*
   Pengujian ini untuk mengehatui kelayakan hasil program berupa *Stego Image* berdasarkan tingkat kemiripan dengan *Cover Image*. *Stego Image* dapat dikatakan layak apabila memiliki nilai PSNR > 40 dB.
d. Pengujian Terhadap Perubahan *Brightness* dan *Contrast*
   Pengujian ini dilakukan untuk membuktikan apakah perubahan pada *brightness* dan *contrast* mempengaruhi isi pesan yang terkandung di dalam stegoimage. Pengujian ini bertujuan mengetahui tingkat kerusakan pesan yang terkandung pada *stegoimage.*
e. Pengujian Terhadap Pemotongan Gambar *(Cropping)*
   Pengujian ini dilakukan untuk membuktikan apakah dengan melakukan pemotongan gambar *(cropping)* dapat mempengaruhi isi pesan yang terkandung di dalam *stegoimage.* Pengujian ini dilakukan dengan memotong stegoimage pada bagian-bagian tertentu. Pengujian ini bertujuan mengetahui tingkat kerusakan pesan yang terkandung pada *stegoimage.*
f. Pengujian Pengiriman *Stegoimage*
   Pengujian ini dilakukan untuk membuktikan apakah pengiriman stegoimage melalui jalur komunikasi pada beberapa aplikasi dapat sampai dengan utuh tanpa mengalami kerusakan berkas. Pengujian ini akan dilakukan dengan cara mengirimkan *stegoimage* melalui beberapa aplikasi, seperti *e-mail*, *line*, dan *whatsapp.*

3. HASIL DAN PEMBAHASAN

3.1. Hasil Penelitian

3.1.1. Analisis Waktu Proses

Berikut adalah data hasil waktu proses enkripsi-embedding dan ekstraksi-dekripsi berdasarkan data uji coba yang digunakan. Data yang tertera adalah rata-rata dari lima kali percobaan.

StatMat
Jurnal Statistika dan Matematika
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

Tabel 3.1 Waktu Proses

Citra Digital	Teks Asli	Angka Prima		Waktu Proses (detik)		
		p	q	Enkripsi - Embedding	Ekstraksi - Dekripsi	Total Waktu
 Logo Unpam (250x250)	MATEMATIKA	7	29	0.038	0.053	0.091
		73	97	0.037	0.092	0.129
		109	131	0.038	0.169	0.207
	MIPA Universitas Pamulang	7	29	0.037	0.052	0.090
		73	97	0.037	0.091	0.128
		109	131	0.037	0.168	0.205
	ABCDEFGHIJKL Mnopqrstuvwx yz1234567890+ -<>	7	29	0.037	0.053	0.090
		73	97	0.038	0.094	0.131
		109	131	0.038	0.145	0.183
 Logo Unpam (500x500)	MATEMATIKA	7	29	0.111	0.205	0.316
		73	97	0.109	0.246	0.355
		109	131	0.112	0.324	0.435
	MIPA Universitas Pamulang	7	29	0.109	0.208	0.317
		73	97	0.109	0.244	0.353
		109	131	0.109	0.319	0.428
	ABCDEFGHIJKL Mnopqrstuvwx yz1234567890+ -<>	7	29	0.109	0.201	0.310
		73	97	0.111	0.243	0.354
		109	131	0.111	0.324	0.435
 Logo Unpam (1000x1000)	MATEMATIKA	7	29	0.339	0.810	1.149
		73	97	0.342	0.848	1.190
		109	131	0.338	0.945	1.283
	MIPA Universitas Pamulang	7	29	0.332	0.808	1.141
		73	97	0.338	0.847	1.185
		109	131	0.333	0.917	1.250
	ABCDEFGHIJKL Mnopqrstuvwx yz1234567890+ -<>	7	29	0.333	0.803	1.136
		73	97	0.336	0.848	1.184
		109	131	0.340	0.945	1.285

Berdasarkan Tabel 3.1, dibuat rangkuman analisis rataan waktu proses berdasarkan masing-masing tipe data.

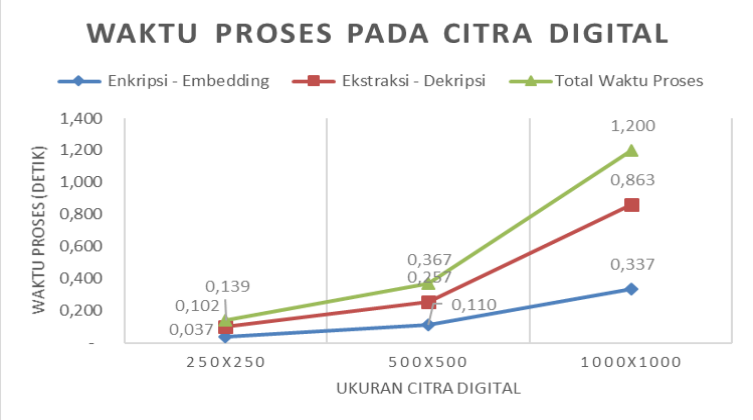
Tabel 3.2 Waktu Proses Tipe Data

Tipe Data	Variasi Data	Rataan Waktu Proses (detik)		Total Waktu Proses (detik)
		Enkripsi - Embedding	Ekstraksi - Dekripsi	
Citra Digital	250x250	0.037	0.102	0.139
	500x500	0.110	0.257	0.367
	1000x1000	0.337	0.863	1.200
Pasangan Angka Prima	1-50	0.160	0.355	0.516
	51-100	0.162	0.395	0.557
	101-150	0.162	0.473	0.635

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

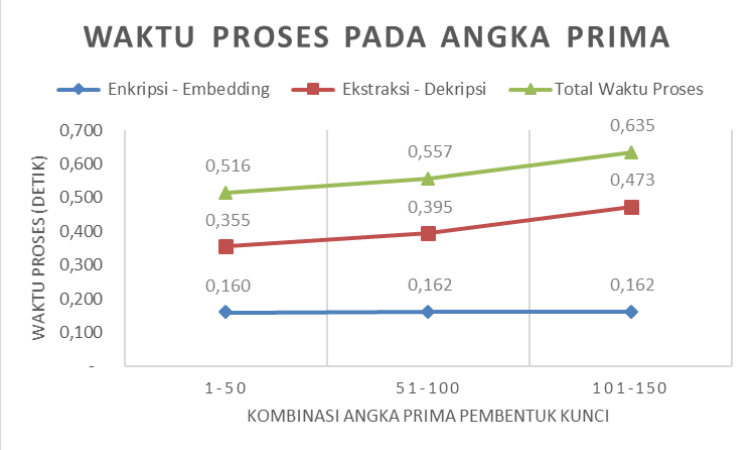
Pesan Digital	10 karakter	0.163	0.410	0.573
	25 karakter	0.160	0.406	0.566
	40 karakter	0.161	0.406	0.568

Dari Tabel 3.2 terlihat bahwa ukuran dari citra digital sangat berpengaruh terhadap waktu proses, baik dalam proses enkripsi-embedding maupun proses ekstraksi-dekripsi. Sedangkan besaran angka prima pembangkit pasangan kunci kurang berpengaruh terhadap waktu proses enkripsi-embedding namun mempengaruhi panjang waktu ekstraksi-dekripsi. Panjangnya pesan digital dalam proses enkripsi-embedding maupun ekstraksi-dekripsi tidak berpengaruh besar terhadap waktu prosesnya. Penyajian Tabel 4.10 dalam bentuk grafik untuk masing-masing tipe data adalah sebagai berikut.



Gambar 3.1 Grafik Hubungan Besarnya Citra Digital Terhadap Waktu Proses

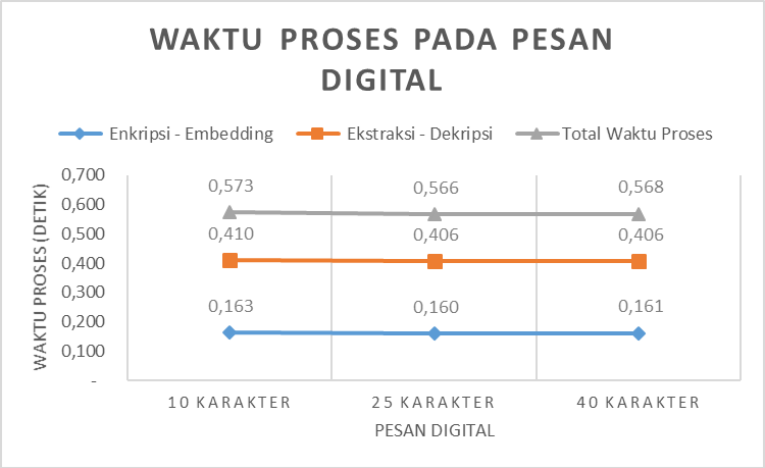
Gambar 3.1 menunjukkan bahwa semakin besar ukuran dari citra maka waktu proses akan semakin lama baik dalam proses enkripsi-embedding maupun proses ekstraksi-dekripsi, hal ini disebabkan karena banyaknya piksel yang harus diproses. Citra yang memiliki ukuran 250x250 piksel dapat diproses dalam waktu 0.139 detik, pada citra berukuran 500x500 piksel dibutuhkan waktu 0.367 detik, dan citra yang memiliki ukuran 1000x1000 piksel membutuhkan waktu proses hingga 1.2 detik.



Gambar 3. 1 Grafik Hubungan Besarnya Angka Prima Terhadap Waktu Proses

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

Gambar 3.2 menunjukkan bahwa pada proses enkripsi-embedding, besarnya angka prima tidak berpengaruh banyak terhadap lama waktunya yang menunnjukkan angka 0.16 detik di masing-masing besaran angka prima. Akan tetapi besaran angka prima cukup berpengaruh pada proses ekstraksi-dekripsi, ditunjukkan pada besaran angka prima 1-50 memerlukan waktu 0.355 detik, besaran angka prima 51-100 memerlukan waktu 0.395 detik, dan meningkat lagi untuk besaran angka prima 101-150 memerlukan waktu proses hingga 0.475 detik. Hal ini membuktikan bahwa benar semakin besar angka prima yang dikombinasikan maka akan semakin sulit untuk diselesaikan, baik secara manual maupun dengan sistem komputasi.



Gambar 3. 2 Grafik Hubungan Panjang Pesan Terhadap Waktu Proses

Gambar 3.3 menunjukkan bahwa panjang pesan digital tidak berpengaruh besar terhadap waktu proses. Terlihat dalam proses enkripsi-embedding baik untuk pesan dengan panjang 10, 25, ataupun 40 karakter memiliki catatan waktu yang relatif sama yaitu 0.16 detik. Begitu pula dengan waktu ekstraksi-dekripsi yang membutuhkan waktu proses yang berkisar diantara 0.4 detik untuk panjang pesan yang berbeda.

3.1.2. Analisis MSE dan PSNR

Berikut adalah data nilai MSE dan PSNR dari *cover image* dan *stego image* berdasarkan data uji coba.

Tabel 3.3 Analisis nilai MSE dan PSNR

Citra Digital	Teks Asli	Angka Prima		MSE	PSNR (dB)
		p	q		
Logo Unpam (250x250)	MATEMATIKA	7	29	0.32071	53.0696
		73	97	0.32069	53.0700
		109	131	0.32061	53.0711
	MIPA Universitas Pamulang	7	29	0.28604	53.5665
		73	97	0.28587	53.5691
		109	131	0.28580	53.5702
		7	29	0.24902	54.1684

StatMat
Jurnal Statistika dan Matematika
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

	ABCDEFGHIJKLMnopqrstuvwxyz1234567890+-<>	73	97	0.24849	54.1778
		109	131	0.24851	54.1774
 Logo Unpam (500x500)	MATEMATIKA	7	29	0.08020	59.0889
		73	97	0.08016	59.0910
		109	131	0.08016	59.0911
	MIPA Universitas Pamulang	7	29	0.07152	59.5863
		73	97	0.07147	59.5898
		109	131	0.07145	59.5907
	ABCDEFGHIJKLMnopqrstuvwxyz1234567890+-<>	7	29	0.06228	60.1877
		73	97	0.06212	60.1985
		109	131	0.06214	60.1969
 Logo Unpam (1000x1000)	MATEMATIKA	7	29	0.02005	65.1095
		73	97	0.02004	65.1116
		109	131	0.02004	65.1117
	MIPA Universitas Pamulang	7	29	0.01789	65.6059
		73	97	0.01787	65.6095
		109	131	0.01786	65.6114
	ABCDEFGHIJKLMnopqrstuvwxyz1234567890+-<>	7	29	0.01557	66.2070
		73	97	0.01553	66.2185
		109	131	0.01554	66.2171

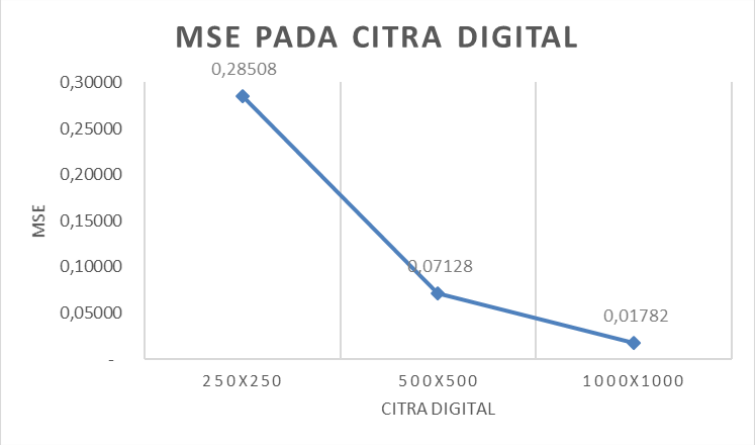
Berdasarkan tabel 3.3, dibuat rangkuman analisis rataan nilai MSE dan PSNR berdasarkan masing-masing tipe data.

Tabel 3.4 Analisis MSE dan PSNR Tipe Data

Tipe Data	Variasi Data	MSE	PSNR (dB)
Citra Digital	250x250	0.28508	53.6045
	500x500	0.07128	59.6245
	1000x1000	0.01782	65.6447
Pasangan Angka Prima	1-50	0.12481	59.6211
	51-100	0.12469	59.6262
	101-150	0.12468	59.6264
Pesan Digital	10 karakter	0.14030	59.0905
	25 karakter	0.12509	59.5888
	40 karakter	0.10880	60.1944

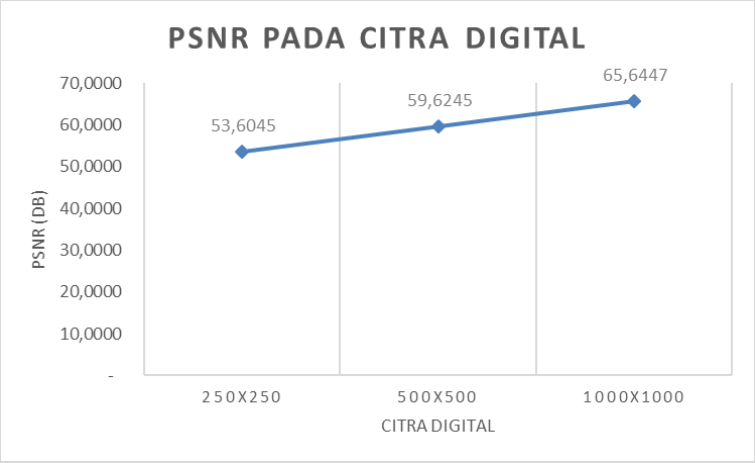
Dari Tabel 3.4 diketahui bahwa nilai MSE dan PSNR paling banyak dipengaruhi oleh ukuran citra, kemudian panjang pesan, namun besaran pasangan angka prima tidak terlalu berpengaruh terhadap nilai dari MSE dan PSNR. Dapat dilihat juga bahwa nilai MSE berbanding terbalik dengan nilai PSNR, semakin kecil nilai MSE maka nilai PSNR akan semakin besar. Penyajian Tabel 3.4 dalam bentuk grafik untuk masing-masing tipe data adalah sebagai berikut.

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam



Gambar 3. 3 Grafik Hubungan Ukuran Citra Terhadap Nilai MSE

Berdasarkan gambar 3.4 dapat diketahui bahwa nilai MSE antara *stego image* dengan *cover image* cenderung menurun pada citra yang berukuran lebih besar. Dapat dilihat bahwa pada citra berukuran 250x250 piksel nilai MSE menunjukkan angka 0.28508, pada citra berukuran 500x500 piksel nilai MSE turun menjadi 0.07128, dan terakhir pada citra berukuran 1000x1000 piksel nilai MSE kembali turun ke angka 0.01782.

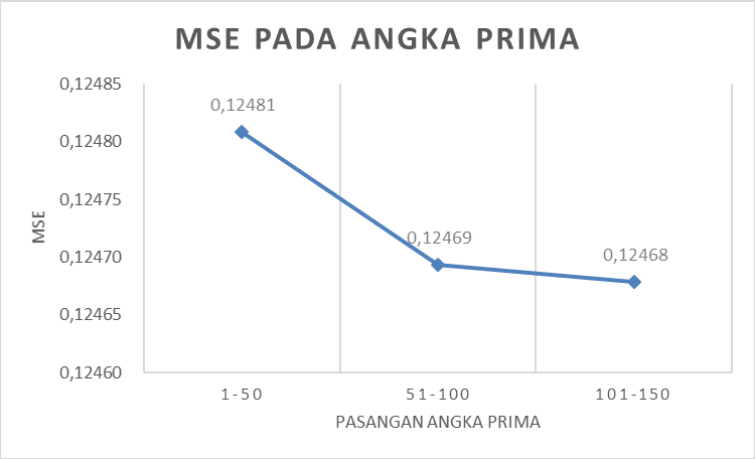


Gambar 3. 4 Grafik Hubungan Ukuran Citra Terhadap Nilai PSNR

Gambar 3.5 menunjukkan bahwa ukuran citra digital mempengaruhi tingkat kemiripan antara *stego image* dengan *cover image*. *Stego Image* dan *Cover image* berukuran 250x250 piksel memiliki nilai PSNR 53.6045 dB, nilai ini sudah dianggap baik karena >40 dB. Untuk citra berukuran 500x500 piksel nilai PSNR meningkat menjadi 59.6245 dB, dan nilai PSNR meningkat lagi pada citra berukuran 1000x1000 piksel dengan nilai 65.6447 dB. Hal ini dipengaruhi karena jumlah piksel yang disisipi pesan

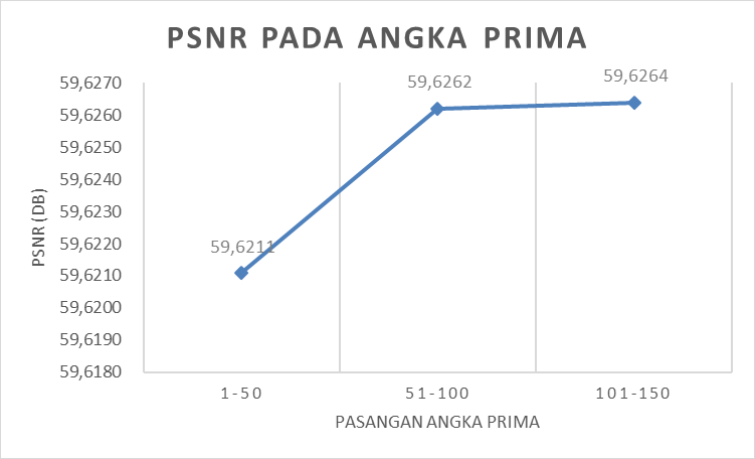
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

tidah berubah sedangkan ukuran gambar meningkat, sehingga rasio piksel yang mengalami perubahan semakin kecil pada gambar yang memiliki ukuran lebih besar.



Gambar 3. 5 Grafik Hubungan Besaran Angka Prima Terhadap Nilai MSE

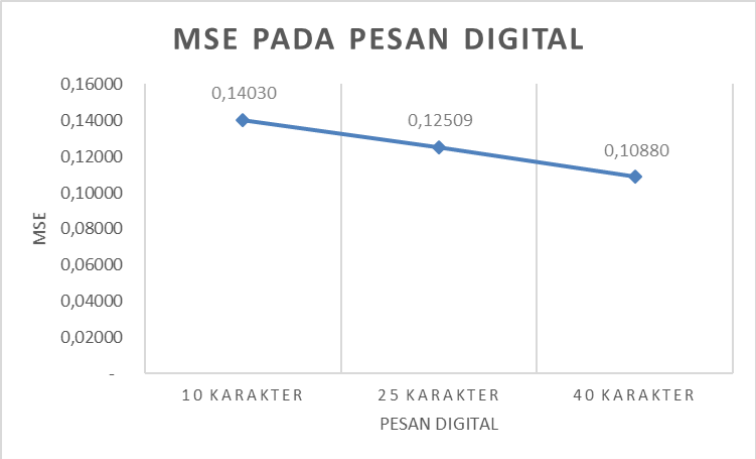
Gambar 3.6 menunjukkan hubungan antara nilai MSE dengan ukuran pasangan angka prima yang digunakan. Dapat dilihat bahwa besaran angka prima yang digunakan sebagai pembangkit kunci hampir tidak berpengaruh terhadap nilai MSE antara *stego image* dengan *cover image*. Untuk pasangan angka prima 1-50 nilai MSE yang didapat adalah 0.12481, untuk pasangan angka prima 51-100 nilai MSE di angka 0.12469, dan untuk pasangan angka prima 101-150 nilai MSE cenderung tetap di angka 0.12468.



Gambar 3. 6 Grafik Hubungan Besaran Angka Prima Terhadap Nilai PSNR

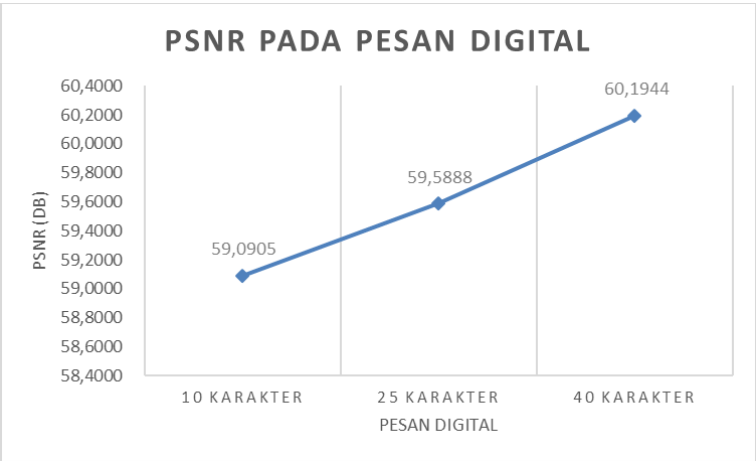
Gambar 3.7 menunjukkan bahwa besaran pasangan angka prima tidak memiliki pengaruh yang cukup besar terhadap nilai PSNR, terlihat pada angka prima 1-50 nilai PSNR 59.6211 dB, pada angka prima 51-100 nilai PSNR cenderung tetap yaitu 59.6262 dB, dan pada agka prima 101-150 nilai PSNR masih berada pada angka 59.6264 dB.

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam



Gambar 3. 7 Grafik Hubungan Panjang Pesan Terhadap Nilai MSE

Gambar 3.8 menunjukkan hubungan antara nilai MSE dengan panjang karakter pesan digital. Dapat dilihat bahwa Panjang karakter pesan digital tidak berpengaruh banyak terhadap nilai MSE. Pesan digital dengan 10 karakter memiliki nilai MSE sebesar 0.1403, pesan digital dengan 25 karakter memiliki nilai MSE turun menjadi 0.12509, dan untuk pesan dengan 40 karakter nilai MSE kembali mengalami penurunan yang tidak signifikan yaitu pada angka 0.1088.



Gambar 3. 8 Grafik Hubungan Panjang Pesan Terhadap Nilai PSNR

Gambar 3.9 menunjukkan bahwa panjang karakter berpengaruh terhadap nilai PSNR. Untuk pesan yang memiliki 10 karakter nilai PSNRnya adalah 59.0905 dB, pesan dengan 25 karakter memiliki nilai PSNR 59.5888 dB, dan pesan dengan 40 karakter nilai PSNRnya kembali meningkat menjadi 60.1944 dB.

StatMat
Jurnal Statistika dan Matematika
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

3.1.3. Analisis Perubahan Citra

Pada bagian ini *stego image* hasil dari proses enkripsi-embedding akan dilakukan perlakuan khusus yaitu penambahan *brightness, contrast,* pemotongan citra secara vertikal dan horisontal, serta perubahan ukuran *(scalling).* Hal ini dilakukan untuk mengetahui ketahanan pesan terhadap perlakuan yang didapat *stego image.*

Tabel 3.5 Analisis Perubahan *Stego Image*

Stego Image	Pesan Asli	Perubahan Pada Stego Image		Pesan Hasil Proses	Ketahanan Pesan
 Logo Unpam Stego (500x500)	MIPA Universitas Pamulang	Brightness +50		□□□□□ □□□□□□ □□□□□□ Pamulang	Rusak
		Contrast +50		□IPA Universitas Pamulang	Rusak
		Crop Vertical		MIPA Universitas Pamulang	Tahan
		Crop Horizontal		MIPA Universitas Pamulang	Tahan
		Scale 1:2		-	Rusak

Dari Tabel 3.5 dapat dilihat bahwa perubahan pada *stego image* dapat mempengaruhi keaslian pesan. Pesan akan rusak jika *stego image* diberi perubahan pada *brightness, contrast,* dan ukuran gambar. Sedangkan pemotongan gambar tidak berpengaruh terhadap keaslian pesan.

3.1.4. Analisis Pengiriman Stego Image

Pada bagian ini *stego image* hasil dari proses enkripsi-embedding akan dikirim melalui beberapa aplikasi pengiriman pesan. Hal ini dilakukan untuk mengetahui ketahanan pesan terhadap pengiriman *stego image* melalui media-media tertentu.

Tabel 3.6 Analisis Pengiriman *Stego Image*

Stego Imaga	Pesan Asli	Media Pengiriman	Pesan Hasil Proses	Ketahanan Pesan
 Logo Unpam Stego (500x500)	MIPA Universitas Pamulang	Email	MIPA Universitas Pamulang	Tahan
		WhatsApp	□□□□□□□□□□ □□□□□□□□□□	Rusak
		Line	MIPA Universitas Pamulang	Tahan

StatMat
Jurnal Statistika dan Matematika
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

Dapat dilihat pada tabel 3.6 bahwa pengiriman *stego image* melalui beberapa media pengiriman pesan dapat merubah pesan asli. Pengiriman dengan menggunakan aplikasi *WhatsApp* mempengaruhi keaslian pesan, sedangkan pengiriman dengan aplikasi *Line* maupun dengan *e-mail* dapat mempertahankan keaslian pesan. Hal ini dipengaruhi karena masing-masing aplikasi pengiriman pesan memiliki penyandian tersendiri pada pesan yang dikirimkan sehingga dapat merubah nilai dari pesan asli.

3.2. Pembahasan

Algoritma kriptografi dan steganografi merupakan metode yang digunakan untuk merahasiakan sebuah pesan agar tidak diketahui pihak yang tidak berhak. Kombinasi algoritma kriptografi RSA dan steganografi LSB meningkatkan keamanan dalam proses penyembunyian pesan. Dalam analisis data diatas digunakan tiga tipe data yaitu citra digital yang digunakan untuk penyisipan pesan pada steganografi, panjang karakter pesan rahasia, dan pasangan angka prima yang digunakan untuk membangkitkan kunci dalam proses enkripsi dan dekripsi.

1. Proses yang terjadi dalam kombinasi algoritma kriptografi RSA dan steganografi LSB terdiri dari proses enkripsi, embedding, ekstraksi, dan dekripsi. Enkripsi merupakan proses perubahan yang dilakukan terhadap pesan rahasia untuk memperoleh pesan acak yang tidak memiliki makna. Embedding merupakan proses dimana pesan acak hasil dari enkripsi disisipkan kedalam sebuah citra dengan memanfaatkan bit terkecil dari masing-masing piksel pada citra. Ekstraksi adalah proses pengembalian pesan dari dalam citra, pesan yang didapat dari hasil ekstraksi masih merupakan pesan acak yang tidak memiliki makna. Dekripsi merupakan proses pengembalian pesan acak yang telah diambil dari dalam *stego image* menjadi bentuk awal sehingga dapat diketahui pesan rahasianya. Algoritma kombinasi yang dihasilkan adalah sebagai berikut :
   a. Algoritma pembangkit kunci
      1) Pilih dua bilangan prima sembarang, p dan q.
      2) Hitung nilai $n=p.q$ (sebaiknya $p \neq q$, karena jika $p = q$ maka $n=p^2$ sehingga nilai p dapat diperoleh dengan menarik akar pangkat dua dari n).
      3) Hitung $\varphi(n) = (p-1).(q-1)$
      4) Pilih kunci e dengan $1 < e < \varphi(n)$ dan e relatif prima terhadap $\varphi(n)$ (gcd (e, $\varphi(n)$) = 1).
      5) Bangkitkan kunci rahasia dengan menggunakan persamaan (2.11).

      Hasil dari algoritma pembangkit kunci adalah :
      1) Kunci umum adalah pasangan (e,n)
      2) Kunci rahasia adalah pasangan (d,n)

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

b. Algoritma enkripsi RSA
   1) Masukkan pesan yang akan dirahasiakan *(plaintext)* (*P*).
   2) Ambil kunci umum *(e,n).*
   3) Nyatakan *plaintext (P)* menjadi blok-blok $P_1, P_2, \ldots, P_i$ sedemikian sehingga setiap blok merepresentasikan nilai [0,n-1].
   4) Setiap blok P_i, dienkripsi menjadi blok C_i dengan persamaan (2.9).

   Hasil dari algoritma ini adalah berupa pesan acak *(ciphertext) (C).*
c. Algoritma embedding LSB
   1) Ubah setiap nilai blok $P_1, P_2, \ldots, P_i$ menjadi bentuk biner 16 bit.
   2) Pilih *cover image* (*I).*
   3) Ubah setiap piksel *cover image I(x,y)* menjadi bentuk biner
   4) Ubah *I(x,y)* menjadi $I_s(x,y)$ dengan persamaan (2.12)

   Hasil dari algoritma ini adalah berupa *stego image* (I_s).
d. Algoritma ekstraksi LSB
   1) Ambil *stego image* (I_s).
   2) Ubah tiap piksel $I_s(x,y)$ menjadi bentuk biner.
   3) Ambil bit terakhir dari setiap piksel.
   4) Susun seluruh bit dan pisahkan menjadi masing-masing 16 bit.
   5) Ubah bentuk biner menjadi nilai [0,n-1].

   Hasil dari algoritma ini adalah berupa *pesan acak (ciphertext) (C).*
e. Algoritma dekripsi RSA
   1) Setiap blok C_i didekripsi menjadi blok P_i dengan persamaan (3.10).
      Hasil dari algoritma ini adalah berupa pesan rahasia *(plaintext) (P).*

2. Bentuk penyandian pada skema steganografi dalam skripsi ini menggunakan algoritma *Least Significant Bit (LSB)* dimana pesan diubah menjadi bentuk biner dan disisipkan ke dalam citra digital dengan mengganti bit terkecil tiap piksel citra tersebut dengan nilai bit pesan. Dalam skema yang digunakan pada skripsi ini pesan yang disisipkan ke dalam citra digital adalah pesan acak hasil dari proes enkripsi pesan asli dalam skema kriptografi RSA. Nilai MSE dan PSNR yang didapat dari hasil perbandingan *cover image* dengan *stego image* cukup bervariasi. Pada kombinasi data pesan 40 karakter, angka prima 51-100, dan citra berukuran 1000x1000 piksel memiliki nilai MSE terendah yaitu 0.01553 akan tetapi menunjukkan nilai PSNR tertinggi yaitu 66.2185 dB. Sedangkan pada kombinasi panjang pesan 10 karakter, angka prima 1-50, dan citra digital ukuran 250x250 piksel diperoleh nilai PSNR terendah yaitu 53.0696 dB dan nilai MSE tertinggi yaitu 0.32071.
3. Tingkat efektifitas akgoritma kombinasi ini disimpulkan dari hasil analisis waktu proses, analisis nilai MSE dan PSNR dan analisis ketahanan pesan terhadap perubahan pada *stego image* serta terhadap pengiriman melalui aplikasi tertentu.

StatMat
Jurnal Statistika dan Matematika
P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

Pada proses analisis waktu disini keempat proses dibagi menjadi dua proses utama yaitu enkripsi-embeddig dan ekstraksi-dekripsi. Proses pertama adalah enkripsi-embedding, dari proses ini dihasilkan *stego image* yang telah disisipi pesan acak dari pesan rahasia. Proses kedua adalah ekstraksi-dekripsi, proses ini mengambil dan mengembalikan pesan rahasia ke bentuk awal. Seperti terliha pada tabel 4.10 jika semakin besar ukuran citra maka waktu proses akan semakin lama, berdasarkan data pada citra berukuran 250x250 piksel, 500x500 piksel, dan 1000x1000 piksel menunjukkan total waktu proses berturut-turut adalah 0.139 detik, 0.367 detik, dan 1.2 detik. Besaran kombinasi angka prima hanya berpengaruh pada proses ekstraksi-dekripsi, pada angka prima dalam interval 1-50, 51-100, dan 100-150 waktu proses enkripsi-embedding cenderung sama di angka 1.16 detik, sedangkan dalam proses ekstraksi-dekripsi berturut-turut waktu prosesnya adalah 0.355 detik, 0.395 detik, dan 0.473 detik. Sedangkan panjang karakter pesan rahasia tidak berpengaruh banyak terhadap waktu proses, waktu enkripsi-embedding cenderung sama di angka 0.16 detik dan waktu ekstraksi-dekripsi juga cenderung statis di angka 0.41 detik untuk panjang 10 karakter, 25 karakter, maupun 40 karakter.

Analisis selanjutnya yang dilakukan adalah analisis nilai MSE dan PSNR. Analisis ini dilakukan untuk mengetahui tingkat kemiripan antara *cover image* dan *stego image*. Dapat dilihat pada tabel 4.12 bahwa nilai MSE berbanding terbalik dengan nilai PSNR. Ukuran citra digital merupakan faktor paling berpengaruh terhadap nilai MSE dan PSNR. Pada citra berukuran 250x250 piksel, 500x500 piksel, dan 1000x1000 piksel nilai MSE berturut-turut adalah 0.28508, 0.07128, dan 0.01782, sedangkan nilai PSNRnya berturut-turut adalah 53.6045 dB, 59.6245 dB, dan 65.6447 dB. Berdasarkan besaran angka prima nilai MSE dan PSNR cenderung sama, nilai MSE berada di angka 0.124 dan PSNR di angka 59.62 dB untuk semua besaran bilangan prima. Panjang pesan hanya sedikit berpengaruh terhadap nilai MSE dan PSNR, dapat dilihat untuk pesan dengan 10, 25, dan 40 karakter nilai MSE berturut-turut adalah 0.1403, 0.12509, dan 0.1088, lalu nilai PSNR berturut-turut 59.0905 dB, 59.5888 dB, dan 60.1944 dB.

Selanjutnya analisis pada ketahanan isi pesan berdasar perlakuan yang diberikan kepada *stego image*. Perlakuan yang diberikan kepada *stego image* yaitu penambahan *brightness, contrast,* pemotongan citra secara vertikal dan horisontal, serta perubahan ukuran *(scalling).* Dapat dilihat pada tabel 4.13 bahwa pesan tidak mengalami kerusakan jika dilakukan pemotongan citra, namun pesan akan rusak jika *stego image* diberi perubahan pada *brightness, contrast*, dan ukuran gambar *(scalling)*. Terakhir adalah analisis ketahanan pesan terhadap pengiriman citra melalui media tertentu. Media yang digunakan pada skripsi ini adalah *e-mail, line*, dan *whatsapp.* Hal ini dilakukan untuk mengetahui media apa yang dapat digunakan untuk mengirimkan *stego image* agar tidak terjadi kerusakan pesan, karena dalam proses pengiriman melalui media tertentu pesan di enkripsi ulang dengan metode

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

yang berbeda. Hasil dari analisis ini dapat dilihat pada tabel 4.14 dimana diketahui bahwa pesan akan tetap utuh jika *stego image* dikirim melalui *e-mail* dan *line*, namun jika *stego image* dikirim melalui *whatsapp* pesan rahasia akan rusak.

4. KESIMPULAN DAN SARAN

4.1. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang sudah dijabarkan dalam bab sebeumnya, dapat disimpulkan sebagai berikut :

1. Bentuk algoritma skema kriptografi dengan menggunakan steganografi dalam skripsi ini menggunakan kombinasi skema kriptografi RSA dan skema steganografi LSB. Pesan yang dirahasiakan dengan menggunakan algoritma mampu direkonstruksi dengan baik. Skema algoritma kombinasi ini disusun dengan menggunakan program Matlab R2015a dan terdiri dari lima proses utama yaitu proses pembangkitan kunci (23 langkah), proses enkripsi (9 langkah), proses embedding (39 langkah), proses ekstraksi (20 langkah), dan proses dekripsi (9 langkah). Kelima proses utama tersebut disusun sedemikan hingga dalam *Graphic User Interface (GUI)* Matlab R2015a dan menghasilkan total 193 langkah.
2. Bentuk penyandian pada skema steganografi dalam skripsi ini menggunakan algoritma *Least Significant Bit (LSB)* dimana pesan diubah menjadi bentuk biner dan disisipkan ke dalam citra digital dengan mengganti bit terkecil tiap piksel citra tersebut dengan nilai bit pesan. Dalam skema yang digunakan pada skripsi ini pesan yang disisipkan ke dalam citra digital dapat direkonstruksi dengan baik. Selain itu nilai PSNR dari semua percobaan menunjukkan angka > 40 dB, nilai *PSNR* terendah 53.0696 dB dan nilai PSNR tertinggi adalah 66.2185 dB. Berdasarkan nilai PSNR dan keaslian pesan yang disembunyikan, menunjukkan bahwa skema ini baik digunakan dalam kombinasi dengan algoritma kriptografi RSA.
3. Analisis efektifitas proses pengamanan pesan digital dengan skema kriptorafi dan steganografi dilakukan dengan menghitung waktu proses program, nilai PSNR, dan ketahanan pesan terhadap perubahan yang dilakukan terhadap *stego image* serta terhadap pengiriman menggunakan beberapa aplikasi. Waktu proses tercepat yang dibutuhkan adalah 0.09 detik dan waktu proses terlama adalah 1.285 detik. Waktu proses lebih banyak dipengaruhi oleh ukuran citra dimana pada citra berukuran 250x250 piksel dibututuhkan waktu proses rata-rata 0.139 detik dan terus meningkat hingga 1.2 detik pada citra berukuran 1000x1000 piksel, sedangkan pasangan angka prima lebih berpengaruh pada waktu ekstraksi-dekripsi dimana pada angka prima 1-50 diperlukan waktu 0.355 detik, angka prima 51-100 diperlukan waktu 0.395 detik, dan tertinggi pada angka prima 100-150 diperlukan waktu 0.473 detik, panjang pesan tidak terlalu berpengaruh terhadap lamanya waktu proses. Nilai PSNR tertinggi adalah 66.2185 dB sedangkan nilai PSNR terendah adalah 53.0696 dB. Sama seperti pada waktu proses, ukuran citra juga

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

paling berpengaruh terhadap nilai PSNR dibandingkan data lain. Pesan dapat rusak jika *stego image* dikenai perlakuan tertentu seperti penambahan *brightness*, *contrast*, dan perubahan ukuran, namun jika *stego image* dipotong baik secara vertikal maupun horisontal, pesan tidak rusak akan tetapi harus diperhatikan juga panjang pesan yang dirahasiakan. Pengiriman *stego image* dapat dilakukan dengan aplikasi *line*, ataupun *e-mail* agar pesan tetap utuh. Dengan analisis tersebut dapat disimpulkan algoritma kombinasi kriptografi RSA dan steganografi LSB cukup efektif digunakan untuk mengamankan pesan digital.

4.2. Saran

Berdasarkan kesimpulan analisis algoritma diatas, dapat dikemukakan saran-saran yang perlu ditindaklanjuti, baik untuk pengembangan pengetahuan, bagi penulis selanjutnya terutama dalam bidang kemananan data, maupun kepentingan praktis. Berikut ini merupakan hal-hal yang perlu ditindaklanjuti tersebut :

1. Pemilihan angka prima dan citra digital sebagai *cover image* sebaiknya disesuaikan dengan panjang pesan dan tingkat kepentingan pesan rahasia.
2. Sebelum mengirim *stego image*, sebaiknya tidak dilakukan perubahan terhadap *stego image* dan dikirim menggunakan *e-mail* atau *line*.
3. Pada penelitian selanjutnya dapat menggunakan metode dan bahasa pemrograman lain agar dapat mengetahui kelemahan dan kelebihan masing-masing metode.
4. Pada penelitian selanjutnya media penampung yang akan disisipkan pesan dapat berupa audio, video ataupun media lain.

5. DAFTAR PUSTAKA

Ariyus, Dony, (2008), *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi*, Andi Publisher, Yogyakarta

Ariyus, Dony, (2009), *Keamanan Multimedia*, Andi Publisher, Yogyakarta

Asih, Nurlita Eka, (2015), *Implementasi Algoritma Least Significant Bit dan Huffman Coding dalam Steganografi Citra Digital*, Skripsi, Universitas Indonesia, Depok.

Karthick, (2013, 3 Maret), *Image Steganography using LSB*, (https://www.mathworks.com/matlabcentral/answers/65679-image-steganography-using-lsb?s_tid=srchtitl, diakses tanggal 26 Juni 2018)

Kromodimoeljo, Sentot, (2010), *Teori & Aplikasi Kriptografi*, SPK IT Consulting, Jakarta

Male, M. G., Wirawan dan Setijadi, E., (2012), *Analisa Kualitas Citra pada Steganografi untuk Aplikasi E-Government*, Seminar Nasional Manajemen Teknologi XV, Surabaya.

Paulus E, Natalia Y, (2007), *Cepat Mahir GUI Matlab*, Andi Publisher, Yogyakarta

Rosen, Kenneth H., (2011), *Elementary Number Theory & Its Applications*, sixth edition, Pearson Education, Boston.

P-ISSN: 2655-3724
STATMAT (Jurnal Statistik dan Matematika), Vol. 1, No. 2, Juli 2019
Halaman: 60-82
@Prodi S-1 Matematika FMIPA Unpam

Santoso, Bekti, (2010), *Kriptografi Visual Untuk Gambar Hitam Putih*, Skripsi, Universitas Indonesia, Depok.

Sianipar, (2017), *Matlab Untuk Mahasiswa*, Andi Publisher, Yogyakarta.

Suprapto, (2008), *Bahasa Pemrograman untuk Sekolah Menengah Kejuruan*, Departemen Pendidikan Nasional, Jakarta.

Sutoyo dkk, (2009), *Teori Pengolahan Citra Digital*, Andi Publisher, Yogyakarta.

Tables, Rapid, ASCII Table, (https://www.rapidtables.com/code/text/ascii-table.html, diakses tanggal 10 Mei 2018)

Wahyudi, Bambang, (2008), *Konsep Sistem Informasi: Dari Bit Sampai Ke Database*, Andi Publisher, Yogyakarta.

Wilms, Vincent, (2015), *RSA Public Key Encryption and Signing*, (https://www.mathworks.com/matlabcentral/fileexchange/53457-rsa-public-key-encryption-and-signing-32bit?s_tid=srchtitle, diakses tanggal 25 Juni 2018)

Wikipedia, (2018, 5 Juni), *ASCII*, (https://id.wikipedia.org/wiki/ASCII, diakses tanggal 19 Agustus 2018)